IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Mark L. Wilkinson, Ronald J. Miller, and Michael J. McDaniels		
Assignee:	Hewlett-Packard Development Company L.P.		
Title:	TRACKING COMMUNICATION FOR DETERMINING DEVICE STATES		
Serial No.:	10/676,541	Filing Date:	October 1, 2003
Examiner:	Truong, ThanhNga B	Group Art Unit:	2135
Docket No.:	1073.P004 US	Confirmation No.:	7659

Irvine, California
May 21, 2008

MAIL STOP APPEAL BRIEFS - PATENTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

APPELLANT'S BRIEF IN RESPONSE TO NOTICE OF NON-COMPLIANT APPEAL BRIEF DATED APRIL 25, 2008

Dear Sir:

This paper is responsive to the Notice Of Non-Compliant Appeal Brief dated April 25, 2008. Reconsideration is respectfully requested.

I. REAL PARTY IN INTEREST

The entire interest in the present application has been assigned to Mirage Networks, Inc., a Delaware corporation having a place of business at 6801 N. Capital of Texas Highway, Austin, TX 78731, at reel 14590 frame 244.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 1-66 are pending in the application. Claims 1-66 are rejected.

The rejections of claims 1-66 are on appeal.

IV. STATUS OF AMENDMENTS

Appellant's Response to the Final Office Action dated August 8, 2007 has been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 pertains to a computer-implemented method comprising observing communication (112, 114) (FIG. 5) (para. [0070]) between a plurality of devices; and inferring a respective state of at least one device of the plurality of devices based upon the observing the communication (FIGs. 17, 18, and 20). The elements of claim 1 are described at least in paragraphs [0064]-[0096], [0115]-[0119], [0132]-[0137] of the specification, and are shown at least in Figures 4, 5, 17, 18, 20, 22, and 23.

Independent claim 31 pertains to a system comprising computer-readable medium encoded with: observing means (338) (FIG. 20) (para. [0113), (112, 114) (FIG. 5) (para. [0070]) for observing communication between a plurality of devices; and inferring means (316-338)(FIG. 5) and (FIGs. 17, 18, and 20) for inferring a respective state of at least one device of the plurality of devices based upon the observing the communication. The elements of claim 31 are described at least in paragraphs [0064]-[0096], [0115]-[0119], [0132]-[0137] of the specification, and are shown at least in Figures 4, 5, 17, 18, 20, 22, and 23.

Independent claim 43 pertains to a system comprising: computer-readable medium encoded with: an observing module (338) (FIG. 20) (para. [0113), (112, 114) (FIG. 5) (para. [0070]) configured to observe communication between a plurality of devices; and an inferring module (316-338)(FIG. 5) and (FIGs. 17, 18, and 20) configured to infer a respective state of at least one device of the plurality of devices based upon the observing the communication. The elements of claim 43 are described at least in paragraphs [0064]-[0096], [0115]-[0119], [0132]-[0137] of the specification, and are shown at least in Figures 4, 5, 17, 18, 20, 22, and 23.

Independent claim 55 pertains to a computer-readable medium encoded with a computer program comprising: observing instructions (338) (FIG. 20) (para. [0113), (112, 114) (FIG. 5) (para. [0070]) configured to observe communication between a plurality of devices; and inferring instructions (316-338)(FIG. 5) and (FIGs. 17, 18, and 20) configured to infer a respective state of at least one device of the plurality of devices based upon the observing the communication. The elements of claim 55 are described at least in paragraphs [0064]-[0096], [0115]-[0119], [0132]-[0137] of the specification, and are shown at least in Figures 4, 5, 17, 18, 20, 22, and 23.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether independent claims 1, 31, 43, and 55 and respective dependent claims 2-30, 32-42, 44-54 and 56-66 are anticipated by Carter *et al.* (US 200310051026), taking into account all limitations of the claims.

VII. ARGUMENT

Rejection of Claims under 35 U.S.C. §102

Claims 1, and 3-12, 14-32, 34-44, 46-56, and 58-66 are rejected under 35 U.S.C. §102(e) as being anticipated by Carter *et al.* (US 200310051026). Claim 1 recites

> "observing communication between a plurality of devices; and
> inferring a respective state of at least one device of the plurality of devices based upon the observing the communication."

In contrast, one cited portion of Carter teaches an Event Learning subcomponent that observes the network's current state of security and incorporates information of a new outcome state that results from an initial known state of security encountering an event which has the potential to change that initial known state. (Carter paragraph [0219]). Claim 1 does not determine the state of the network, but rather a respective state for at least one of the devices. At least one device is assigned its own respective state in claim 1, whereas Carter only determines the security status of the network.

Another cited portion of Carter teaches developing separate populations of problem solving processes by application of co-evolution, and determining the fitness of the constituents of the separate populations. (Carter paragraph [0242]). The determination of the constituents' fitness is based on their ability to accomplish specified results and on prior observations of network events. (Carter, *Id.*). Nothing in Carter discloses or suggests that a respective state is inferred for at least one device based upon the observing the communication between a plurality of devices as set forth in claim 1. Carter only determines the fitness of constituents based on their ability to accomplish specified results, not devices among which communication is being observed as set forth in claim 1.

The Examiner further cited paragraph [0207] of Carter as teaching inferring the respective state of a device. Appellant respectfully disagrees. The cited portion of

Carter defines "stateful" as keeping track of the state of a sequence of interactions with a user, another computer or program, a device, or other outside element. Keeping track of the interaction between elements in Carter is not the same as inferring a state of at least one device based upon observing communication between a plurality of devices in claim 1.

Claim 1 is distinguishable from Carter for at least these reasons.

Claims 2-30 depend from claim 1 and include features that further distinguish them from the prior art. For example, claim 9 recites:

> "setting a designation for a first device of the at least one device to a possible threat based upon a packet configuration for a packet sent by the first device as part of the communication".

In contrast, paragraph [0787] of Carter teaches a list of observations made by the Network Surveillance and Security System. None of the observation events describe designating a device as a possible threat based upon the packet configuration sent by the device. Instead, Carter teaches determining the current security status of a system and predicting the future state of the system based on past security states. (Carter paragraphs [0260]-[0261]). Since Carter does not disclose or suggest setting or predicting a designation for a device based upon a packet configuration for a packet sent by the device, Claim 9 is distinguishable from the prior art for at least these additional reasons.

As a further example, claim 13 recites:

> "the respective state of the first device is determined to be unfulfilled when the observing the communication comprises
> observing an address resolution protocol request comprising a destination address for the first device, and
> observing that the first device does not respond to the address resolution protocol request prior to expiration of a time limit".

The cited portions of Carter do not disclose or suggest these features. Rather, Carter teaches TCP/IP functions of assembling messages into packets for transmission over a network. (Carter paragraph [0028]). (See Carter paragraph [0060] for a diagram of the OSI Reference Model with TCP/IP protocols in network layers 4 and 3, respectively). Another cited portion of Carter describes a frame of data that is transmitted between network points complete with addressing and protocol control information. (Carter paragraph [0084]). Yet another cited portion of Carter describes operation of the Internet Protocol (IP). (Carter paragraph [0152]). Appellant has also reviewed Carter's teaching of identifying potential threats and resulting state transitions for a protected server constellation, as described by paragraphs [785]-[0866] and Figure 19, and paragraphs [1073]-[1090] and Figure 20 in Carter. Appellant finds no indication that Carter discloses or suggests changing the state of the first device when the first device does not respond to the address resolution protocol request prior to expiration of a time limit. Claim 13 is distinguishable from Carter for at least these reasons.

As another example, claim 23 recites:

> "wherein the respective state of the first device is determined to be omitted when the observing is programmed to omit communication with the first device from the observing."

Nothing in Carter teaches or suggests these features. One cited portion of Carter teaches that the NAI Learning component hypothesizes a theorem about the security state of the protected constellation, determines the validity of the theorem by comparing with observations, and incorporates into the knowledge base as facts those theorems which prove valid. (Carter paragraph [0461]). Another cited portion of Carter teaches use of Unix commands to obtain information relating to any user of the protected constellation. The information about the users is retrieved from the results of the constellation traffic audits. (Carter paragraph [0870]). Some of the default values of the commands are set to ignore the respective event, but the traffic audits are still performed for the device regardless of whether the events are ignored. (Carter paragraph [0966]). Carter thus does not teach or suggest the features of the state of the device being determined as omitted as set forth in claim 23.

Claims 31-42 were rejected with the same rationale applied against claims 1, 10-11, 13-14, 16-17, 19, 21, 23, and 26-27. Claims 31-42 are distinguishable from the cited references for at least the same respective reasons provided for the claims 1, 13, and 23 above.

Claims 43-54 were rejected with the same rationale applied against claims 1, 10-11, 13-14, 16-17, 19, 21, 23, and 26-27. Claims 43-54 are distinguishable from the cited references for at least the same respective reasons provided for the claims 1, 13, and 23 above.

Claims 55-66 were rejected with the same rationale applied against claims 1, 10-11, 13-14, 16-17, 19, 21, 23, and 26-27. Claims 55-66 are distinguishable from the cited references for at least the same respective reasons provided for the claims 1, 13, and 23 above.

I hereby certify that this correspondence is being transmitted to the USPTO on the date shown below:

/Mary Jo Bertani/
(Signature)

Mary Jo Bertani
(Printed Name of Person Signing Certificate)

May 21, 2008
(Date)

Respectfully submitted,

/Mary Jo Bertani/

Mary Jo Bertani
Attorney for Appellant(s)
Reg. No. 42,321

VIII. CLAIMS APPENDIX

Claims remaining in the application are as follows:

1. (Previously presented): A computer-implemented method comprising:
observing communication between a plurality of devices; and
inferring a respective state of at least one device of the plurality of devices based upon the observing the communication.

2. (Original): The method of claim 1 wherein
the inferring is performed without sending a packet to the at least one device.

3. (Original): The method of claim 1 wherein
the inferring is performed without participating in the communication with the at least one device.

4. (Original): The method of claim 1 wherein
the inferring is performed only by listening to the communication with the at least one device.

5. (Original): The method of claim 1 further comprising:
setting a designation for a first device of the plurality of devices to a threat when the first device receives a packet and
the respective state of the first device is unfulfilled.

6. (Original): The method of claim 5 further comprising:
changing the designation for the first device to a non-threat when subsequent communication initiated by the first device does not violate a rule for the communication.

7. (Original): The method of claim 1 further comprising:
setting a designation for a first device of the plurality of devices to a possible threat when
the communication is initiated by the first device, and

the communication initiated by the first device violates a rule.

8. (Original): The method of claim 7 further comprising:
changing the designation for the first device to a non-threat when subsequent communication initiated by the first device does not violate a second rule for the communication.

9. (Original): The method of claim 1 further comprising:
setting a designation for a first device of the at least one device to a possible threat based upon a packet configuration for a packet sent by the first device as part of the communication.

10. (Original): The method of claim 1 wherein
the respective state of a first device of the at least one device is determined to be unknown.

11. (Original): The method of claim 10 wherein
the respective state of the first device is determined to be unknown when the observing the communication comprises
observing that the first device fails to respond to the communication sent to the first device.

12. (Original): The method of claim 1 wherein
the respective state of a first device of the at least one device is determined to be unfulfilled.

13. (Original) The method of claim 12 wherein
the respective state of the first device is determined to be unfulfilled when the observing the communication comprises
observing an address resolution protocol request comprising a destination address for the first device, and
observing that the first device does not respond to the address resolution protocol request prior to expiration of a time limit

14. (Original): The method of claim 12 wherein
the respective state of the first device is determined to be unfulfilled when the first device receives an address resolution protocol request.

15. (Original): The method of claim 1 wherein
the respective state of a first device of the plurality of devices is determined to be used.

16. (Original): The method of claim 15 wherein
the respective state of the first device is determined to be used when the observing the communication comprises
observing that the first device performs one of sending and receiving a packet.

17. (Original): The method of claim 15 wherein
the respective state of the first device is determined to be used when the observing the communication comprises
observing that the first device received a packet when the respective state for the first device was unfulfilled, and
observing that the first device sent a reply to the packet within a time limit.

18. (Original): The method of claim 1 wherein
the respective state of a first device of the plurality of devices is determined to be virtual.

19. (Original): The method of claim 18 wherein
the respective state of the first device is determined to be virtual when the observing the communication comprises
observing that the first device received a packet when the respective state for the first device was unfulfilled, and
observing that the first device did not send a reply to the packet within a time limit.

20. (Original): The method of claim 1 wherein
the respective state of a first device of the plurality of devices is determined to be automatic.

21. (Original): The method of claim 20 wherein
the respective state of the first device is determined to be automatic when
an automatic reply is programmed to be sent to a second address when the first device receives a packet from the second address.

22. (Original): The method of claim 1 wherein
the respective state of the first device is determined to be omitted.

23. (Original): The method of claim 22 wherein
the respective state of the first device is determined to be omitted when
the observing is programmed to omit communication with the first device from the observing.

24. (Original): The method of claim 1 further comprising:
initializing the respective state of at least one device of the plurality of devices to unknown prior to the observing.

25. (Original): The method of claim 1 wherein
the plurality of devices communicates via a segment of a network.

26. (Original): The method of claim 1 further comprising:
maintaining the respective state for one device of the at least one device in a storage area.

27. (Original): The method of claim 1 wherein
storing information about at least one packet of a plurality of packets communicated between the plurality of devices.

28. (Original): The method of claim 27 wherein
the information comprises a respective source address and a respective destination address for each packet of the plurality of packets.

29. (Original): The method of claim 27 wherein
the information comprises a protocol for each packet of the plurality of packets.

30. (Original): The method of claim 27 wherein
the information comprises a time that each packet of the plurality of packets was sent.

31. (Previously presented): A system comprising:
tangible computer-readable medium encoded with:
observing means for observing communication between a plurality of devices; and
inferring means for inferring a respective state of at least one device of the plurality of devices based upon the observing the communication.

32. (Previously presented): The system of claim 31 further comprising:
tangible computer-readable medium encoded with:
determining means for determining that the respective state is unknown when the observing the communication comprises
observing that the first device fails to respond to the communication sent to the first device.

33. (Previously presented): The system of claim 31 further comprising:
tangible computer-readable medium encoded with:
determining means for determining that the respective state of the first device is unfulfilled when the observing the communication comprises
observing an address resolution protocol request comprising a destination address for the first device, and
observing that the first device does not respond to the address resolution protocol request prior to expiration of a time limit.

34. (Previously presented): The system of claim 31 further comprising:
tangible computer-readable medium encoded with:
determining means for determining that the respective state of the first device is unfulfilled when the first device receives an address resolution protocol request.

35. (Previously presented): The system of claim 31 further comprising:
tangible computer-readable medium encoded with:

determining means for determining that the respective state of the first device is used when the observing the communication comprises

observing that the first device performs one of sending and receiving a packet.

36. (Previously presented): The system of claim 31 further comprising:

tangible computer-readable medium encoded with:

determining means for determining that the respective state of the first device is used when the observing the communication comprises

observing that the first device received a packet when the respective state for the first device wais unfulfilled, and

observing that the first device sent a reply to the packet within a time limit.

37. (Previously presented): The system of claim 31 further comprising:

tangible computer-readable medium encoded with:

determining means for determining that the respective state of a first device of the plurality of devices is virtual when the observing the communication comprises

observing that the first device received a packet when the respective state for the first device was unfulfilled, and

observing that the first device failed to send a reply to the packet within a time limit.

38. (Previously presented): The system of claim 31 further comprising:

tangible computer-readable medium encoded with:

determining means for determining that the respective state of the first device is automatic when

an automatic reply is programmed to be sent to a second address when the first device receives a packet from the second address.

39. (Previously presented): The system of claim 31 further comprising:

tangible computer-readable medium encoded with:

determining means for determining that the respective state of the first device is omitted when

the observing is programmed to omit communication with the first device from the observing.

40. (Previously presented): The system of claim 31 further comprising:
tangible computer-readable medium encoded with:
initializing means for initializing the respective state of at least one device of the plurality of devices to unknown prior to the observing.

41. (Previously presented): The system of claim 31 further comprising:
tangible computer-readable medium encoded with:
maintaining means for maintaining the respective state for one device of the at least one device in a storage area.

42. (Previously presented): The system of claim 31 further comprising:
tangible computer-readable medium encoded with:
storing means for storing information about at least one packet of a plurality of packets communicated between the plurality of devices.

43. (Previously presented): A system comprising:
tangible computer-readable medium encoded with:
an observing module configured to observe communication between a plurality of devices; and
an inferring module configured to infer a respective state of at least one device of the plurality of devices based upon the observing the communication.

44. (Previously presented): The system of claim 43 wherein the computer-readable medium is further encoded with:
a determining module configured to determine that the respective state is unknown when the observing the communication comprises
observing that the first device fails to respond to the communication sent to the first device.

45. (Previously presented): The system of claim 43 wherein the computer-readable medium is further encoded with:

a determining module configured to determine that the respective state of the first device is unfulfilled when the observing the communication comprises

observing an address resolution protocol request comprising a destination address for the first device, and

observing that the first device does not respond to the address resolution protocol request prior to expiration of a time limit.

46. (Previously presented): The system of claim 43 wherein the computer-readable medium is further encoded with:

a determining module configured to determine that the respective state of the first device is unfulfilled when the first device receives an address resolution protocol request.

47. (Previously presented): The system of claim 43 wherein the computer-readable medium is further encoded with:

a determining module configured to determine that the respective state of the first device is used when the observing the communication comprises

observing that the first device performs one of sending and receiving a packet.

48. (Previously presented): The system of claim 43 wherein the computer-readable medium is further encoded with:

a determining module configured to determine that the respective state of the first device is used when the observing the communication comprises

observing that the first device received a packet when the respective state for the first device wais unfulfilled, and

observing that the first device sent a reply to the packet within a time limit.

49. (Previously presented): The system of claim 43 wherein the computer-readable medium is further encoded with:

a determining module configured to determine that the respective state of a first device of the plurality of devices is virtual when the observing the communication comprises

observing that the first device received a packet when the respective state for the first device was unfulfilled, and

observing that the first device failed to send a reply to the packet within a time limit.

50. (Previously presented): The system of claim 43 wherein the computer-readable medium is further encoded with:

a determining module configured to determine that the respective state of the first device is automatic when

an automatic reply is programmed to be sent to a second address when the first device receives a packet from the second address.

51. (Previously presented): The system of claim 43 wherein the computer-readable medium is further encoded with:

a determining module configured to determine that the respective state of the first device is omitted when

the observing is programmed to omit communication with the first device from the observing.

52. (Previously presented): The system of claim 43 wherein the computer-readable medium is further encoded with:

an initializing module configured to initialize the respective state of at least one device of the plurality of devices to unknown prior to the observing.

53. (Previously presented): The system of claim 43 wherein the computer-readable medium is further encoded with:

a maintaining module configured to maintain the respective state for one device of the at least one device in a storage area.

54. (Previously presented): The system of claim 43 wherein the computer-readable medium is further encoded with:

a storing module configured to store information about at least one packet of a plurality of packets communicated between the plurality of devices.

55. (Previously presented): A tangible computer-readable medium encoded with a computer program comprising:

observing instructions configured to observe communication between a plurality of devices; and

inferring instructions configured to infer a respective state of at least one device of the plurality of devices based upon the observing the communication.

56. (Original): The computer-readable medium of claim 55 further comprising:

determining instructions configured to determine that the respective state is unknown when the observing the communication comprises

observing that the first device fails to respond to the communication sent to the first device.

57. (Original): The computer-readable medium of claim 55 further comprising:

determining instructions configured to determine that the respective state of the first device is unfulfilled when the observing the communication comprises

observing an address resolution protocol request comprising a destination address for the first device, and

observing that the first device does not respond to the address resolution protocol request prior to expiration of a time limit.

58. (Original): The computer-readable medium of claim 55 further comprising:

determining instructions configured to determine that the respective state of the first device is unfulfilled when the first device receives an address resolution protocol request.

59. (Original): The computer-readable medium of claim 55 further comprising:

determining instructions configured to determine that the respective state of the first device is used when the observing the communication comprises

observing that the first device performs one of sending and receiving a packet.

60. (Original): The computer-readable medium of claim 55 further comprising:

determining instructions configured to determine that the respective state of the first device is used when the observing the communication comprises

observing that the first device received a packet when the respective state for the first device wais unfulfilled, and

observing that the first device sent a reply to the packet within a time limit.

61. (Original): The computer-readable medium of claim 55 further comprising:

determining instructions configured to determine that the respective state of a first device of the plurality of devices is virtual when the observing the communication comprises

observing that the first device received a packet when the respective state for the first device was unfulfilled, and

observing that the first device failed to send a reply to the packet within a time limit.

62. (Original): The computer-readable medium of claim 55 further comprising:

determining instructions configured to determine that the respective state of the first device is automatic when

an automatic reply is programmed to be sent to a second address when the first device receives a packet from the second address.

63. (Original): The computer-readable medium of claim 55 further comprising:

determining instructions configured to determine that the respective state of the first device is omitted when

the observing is programmed to omit communication with the first device from the observing.

64. (Original): The computer-readable medium of claim 55 further comprising:

initializing instructions configured to initialize the respective state of at least one device of the plurality of devices to unknown prior to the observing.

65. (Original): The computer-readable medium of claim 55 further comprising:

maintaining instructions configured to maintain the respective state for one device of the at least one device in a storage area.

66. (Original): The computer-readable medium of claim 55 further comprising:

storing instructions configured to store information about at least one packet of a plurality of packets communicated between the plurality of devices.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.